

Rundschreiben 2008/24

Überwachung und interne Kontrolle Banken

Überwachung und interne Kontrolle bei Banken

Referenz: FINMA-RS 08/24 „Überwachung und interne Kontrolle Banken“
 Erlass: 20. November 2008
 Inkraftsetzung: 1. Januar 2009
 Letzte Änderung: 20. November 2008
 Konkordanz: vormals EBK-RS 06/6 „Überwachung und interne Kontrolle“ vom 27. September 2006
 Rechtliche Grundlagen: FINMAG Art. 7 Abs. 1 Bst. b
 BankG Art. 3 Abs. 2 Bst. a, 3b–3g, 4^{quinquies}
 BankV Art. 8 Abs. 2, 9
 BEHG Art. 10 Abs. 2 Bst. a und Abs. 5, 14
 BEHV Art. 19, 20, 29
 ERV Art. 6–11

| Adressaten | | | | | | | | | | | | | | | | | | | | | | |
|------------|---------------------------|---------------------|-------------|---------------------------|------------|-----------------------|---------------|----------------|-------|------------|-------|-------------|------------------------|-----------------|---------------------|---------------------|-----|------|-------------------|------------------------|-----------------|--|
| BankG | | | VAG | | | BEHG | | KAG | | | | | | GwG | | Andere | | | | | | |
| Banken | Finanzgruppen und -kongl. | Andere Intermediäre | Versicherer | Vers.-Gruppen und -Kongl. | Vermittler | Börsen und Teilnehmer | Effekthändler | Fondsleitungen | SICAV | KG für KKA | SICAF | Depotbanken | Vermögensverwalter KKA | Vertriebsträger | Vertreter ausl. KKA | Andere Intermediäre | SRO | DUFU | SRO-Beaufichtigte | Prüfungsgesellschaften | Ratingagenturen | |
| X | X | | | | | | X | | | | | | | | | | | | | | | |

| | | |
|--|----|-------|
| I. Gegenstand | Rz | 1–2 |
| II. Geltungsbereich | Rz | 3–8 |
| III. Verwaltungsrat | Rz | 9–53 |
| A. Aufgaben und Verantwortlichkeiten | Rz | 9–16 |
| a) Überwachung und interne Kontrolle | Rz | 9–11 |
| b) Kontrollumfeld | Rz | 12–14 |
| c) Einrichtung und Überwachung der internen Revision | Rz | 15–16 |
| B. Mitglieder des Verwaltungsrats | Rz | 17–27 |
| a) Allgemeine Voraussetzungen | Rz | 17 |
| b) Unabhängigkeit | Rz | 18–27 |
| C. Arbeitsteilung im Verwaltungsrat und Ausschüsse des Verwaltungsrats | Rz | 28–31 |
| D. Audit Committee | Rz | 32–53 |
| a) Kriterien bezüglich Einrichtung eines Audit Committee | Rz | 32–37 |
| b) Anforderungen an die Mitglieder des Audit Committee | Rz | 38–40 |
| c) Aufgaben eines Audit Committee | Rz | 41–53 |
| aa) <i>Überwachung und Beurteilung der Integrität der Finanzabschlüsse</i> | Rz | 42–44 |
| bb) <i>Überwachung und Beurteilung der internen Kontrolle im Bereich der finanziellen Berichterstattung</i> | Rz | 45–46 |
| cc) <i>Überwachung und Beurteilung der Wirksamkeit der Prüfgesellschaft sowie deren Zusammenwirken mit der internen Revision</i> | Rz | 47–51 |
| dd) <i>Beurteilung der über den Bereich der finanziellen Berichterstattung hinausgehenden internen Kontrolle und der internen Revision</i> | Rz | 52–53 |
| IV. Interne Revision | Rz | 54–79 |
| A. Einrichtung | Rz | 54–59 |
| B. Unterstellung und Organisation | Rz | 60–68 |

| | | | |
|------------|---|----|---------|
| C. | Aufgaben und Verantwortlichkeiten | Rz | 69–79 |
| a) | Risikobeurteilung, Prüfplanung und Berichterstattung | Rz | 69–77 |
| b) | Abgrenzung zur Prüfgesellschaft | Rz | 78–79 |
| V. | Geschäftsführung | Rz | 80–126 |
| A. | Aufgaben und Verantwortlichkeiten | Rz | 80–85 |
| B. | Funktionentrennung und Kontrollaktivitäten | Rz | 86–96 |
| C. | Compliance (Normeneinhaltung) | Rz | 97–99 |
| D. | Compliance-Funktion | Rz | 100–112 |
| a) | Einrichtung und Unterstellung | Rz | 100–106 |
| b) | Aufgaben und Verantwortlichkeiten | Rz | 107–112 |
| E. | Risikokontrolle | Rz | 113–126 |
| a) | Einrichtung und Unterstellung | Rz | 113–120 |
| b) | Aufgaben und Verantwortlichkeiten | Rz | 121–125 |
| c) | Abgrenzung zum Risikomanagement | Rz | 126 |
| VI. | Prüfung und Beurteilung durch die Prüfgesellschaften | Rz | 127 |

I. Gegenstand

Das vorliegende Rundschreiben macht Vorgaben zur Corporate Governance, zur Überwachung der Geschäftstätigkeit und zur internen Kontrolle und deren Überwachung durch die zuständigen Stellen in Banken, Effekthändlern, Finanzgruppen (Art. 3c Abs. 1 des Bankengesetzes [BankG; SR 952.0]) und bank- oder effektenhandelsdominierten Finanzkonglomeraten (Art. 3c Abs. 2 BankG). Diese werden nachfolgend als Institute bezeichnet. 1

Die interne Kontrolle (Synonym internes Kontrollsystem) umfasst die Gesamtheit der Kontrollstrukturen und -prozesse, welche auf allen Ebenen des Instituts die Grundlage für die Erreichung der geschäftspolitischen Ziele und einen ordnungsgemässen Institutsbetrieb bilden. Dabei beinhaltet die interne Kontrolle nicht nur Aktivitäten der nachträglichen Kontrolle, sondern auch solche der Planung und Steuerung. Eine wirksame interne Kontrolle umfasst u. a. in die Arbeitsabläufe integrierte Kontrollaktivitäten, Prozesse für Risikomanagement und Einhaltung der anwendbaren Normen (Compliance), eine von der Risikobewirtschaftung unabhängige Risikokontrolle sowie die Compliance-Funktion. Die interne Revision prüft und beurteilt die interne Kontrolle und trägt dadurch zu deren laufenden Verbesserung bei. 2

II. Geltungsbereich

Das Rundschreiben gilt für Institute gemäss Rz 1, mit folgenden Einschränkungen: 3

- Effekthändler ohne Bankenstatus: Erfolgt bei diesen keine personelle Trennung zwischen Verwaltungsrat und Geschäftsführung, so finden Rz 18–40 keine Anwendung. Rz 41–53 finden sinngemäss Anwendung. 4
- Privatbankiers: Rz 18–40 finden keine Anwendung. Rz 41–53 finden sinngemäss Anwendung. Von den übrigen Bestimmungen sind, nach Absprache mit der Prüfgesellschaft und FINMA, Abweichungen und Vereinfachungen solange zulässig, als die Partner die Merkmale der persönlichen Haftung und Führung der Geschäfte aufweisen. 5
- Direkt und indirekt gehaltene Tochterbanken und Effekthändler sowie hauptsächlich im Finanzbereich tätige Tochterunternehmen von in- und ausländischen Finanzgruppen und bank- oder effektenhandelsdominierten Finanzkonglomeraten: Rz 18–40 finden keine Anwendung, die Einrichtung eines Audit Committee wird aber empfohlen. Rz 41–53 finden sinngemäss Anwendung. 6
- Zweigniederlassungen ausländischer Institute: Rz 9–53 finden keine Anwendung. Die übrigen Bestimmungen finden sinngemäss Anwendung. 7
- Nicht hauptsächlich im Finanzbereich tätige Unternehmen in Finanzgruppen und bank- oder effektenhandelsdominierten Finanzkonglomeraten: Das Rundschreiben findet keine Anwendung. In Zweifelsfällen können bestimmte Konzerngesellschaften auf Antrag der Muttergesellschaft explizit von der Anwendung des Rundschreibens ausgenommen werden. 8

III. Verwaltungsrat

A. Aufgaben und Verantwortlichkeiten

a) Überwachung und interne Kontrolle

Der Verwaltungsrat, d.h. das Organ für Oberleitung, Aufsicht und Kontrolle, trägt die Verantwortung für die Reglementierung, Einrichtung, Aufrechterhaltung, Überwachung und regelmässige Überprüfung einer angemessenen internen Kontrolle, welche der Grösse, der Komplexität, der Struktur und dem Risikoprofil des Instituts angepasst ist. 9

Durch die aus einer systematischen Risikoanalyse abgeleitete interne Kontrolle und deren Überwachung stellt der Verwaltungsrat sicher, dass alle wesentlichen Risiken im Institut erfasst, begrenzt und überwacht werden. In Finanzgruppen und bank- oder effektenhandelsdominierten Finanzkonglomeraten sind besonders auch die Risiken, welche sich aus dem Zusammenschluss mehrerer Unternehmen zu einer wirtschaftlichen Einheit ergeben, zu berücksichtigen. Die systematische Risikoanalyse ist schriftlich zu dokumentieren. 10

Der Verwaltungsrat erörtert mit der Geschäftsführung regelmässig deren Einschätzung über die Angemessenheit und Wirksamkeit der internen Kontrolle. 11

b) Kontrollumfeld

Der Verwaltungsrat sorgt mit seinen Vorgaben an die Geschäftsführung dafür, dass die Mitarbeiter aller Hierarchiestufen ihre Verantwortung und Aufgaben im Prozess der internen Kontrolle kennen und verstehen. 12

Der Verwaltungsrat stellt sicher, dass ein allenfalls auf die Mitarbeiter aller Hierarchiestufen ausgeübter Druck zur Erreichung von Zielvorgaben nicht zur Umgehung von Kontrollmechanismen führen darf. Er sorgt dafür, dass die Entschädigungssysteme keine Anreize zur Missachtung interner Kontrollmechanismen bieten. 13

Der Verwaltungsrat sorgt dafür, dass der Umgang mit Interessenkonflikten geregelt wird. Lässt sich ein Interessenkonflikt im Einzelfall nicht vermeiden, trifft das Institut Massnahmen zur Behandlung des Interessenkonflikts. 14

c) Einrichtung und Überwachung der internen Revision

Der Verwaltungsrat richtet eine interne Revision ein, welche ihm oder dem Audit Committee (bzw. einem anderen Ausschuss) direkt unterstellt ist. Zu Organisation, Aufgaben und Verantwortlichkeiten sowie Rechenschafts- und Berichterstattungspflichten siehe Rz 54–79. 15

Der Verwaltungsrat oder der zuständige Ausschuss überwacht und beurteilt die interne Revision und vergewissert sich periodisch, dass diese über angemessene Ressourcen und Kompetenzen sowie Unabhängigkeit und Objektivität verfügt, um ihre Prüfaufgaben beim Institut wahrzunehmen. 16

B. Mitglieder des Verwaltungsrats

a) Allgemeine Voraussetzungen

Zur Wahrnehmung seiner Aufgaben muss der Verwaltungsrat als Gremium die dafür notwendigen Voraussetzungen, insbesondere Fachkenntnisse, Erfahrung und zeitliche Verfügbarkeit, aufweisen. Er beurteilt mindestens jährlich seine Zielerreichung und Arbeitsweise und dokumentiert dies schriftlich. 17

b) Unabhängigkeit

Die Mitglieder des Verwaltungsrats ordnen ihre persönlichen und geschäftlichen Verhältnisse grundsätzlich so, dass Interessenkonflikte mit dem Institut möglichst vermieden werden. Insbesondere ist es Verwaltungsratsmitgliedern gemäss Art. 8 Abs. 2 BankV untersagt, gleichzeitig der Geschäftsführung des Instituts anzugehören. 18

Der Verwaltungsrat sollte mindestens zu einem Drittel aus Mitgliedern bestehen, welche die Unabhängigkeitskriterien nach Rz 20–24 erfüllen. Diese Mitglieder sind im Jahresbericht mit Namen aufzuführen. Erfüllen weniger als ein Drittel der Mitglieder die Anforderungen an die Unabhängigkeit, ist dies im Jahresbericht zu begründen. 19

Ein Mitglied des Verwaltungsrats gilt als unabhängig, wenn es mindestens die folgenden Kriterien erfüllt: 20

- nicht in anderer Funktion beim Institut beschäftigt ist und dies auch nicht innerhalb der letzten 2 Jahre gewesen ist; 21
- innerhalb der letzten 2 Jahre nicht bei der Prüfgesellschaft des Instituts als für das Institut verantwortlicher leitender Prüfer beschäftigt gewesen ist; 22
- keine geschäftliche Beziehung zum Institut aufweist, welche aufgrund ihrer Art oder ihres Umfangs zu einem Interessenkonflikt führt; und 23
- nicht qualifizierter Beteiligter (im Sinne von Art. 3 Abs. 2 Bst. c^{bis} BankG und Art. 10 Abs. 2 Bst. d BEHG) des Instituts ist und auch keinen solchen vertritt. 24

Von Kantonen, Gemeinden oder anderen kantonalen oder kommunalen Anstalten des öffentlichen Rechts in den Verwaltungsrat von Kantonal- oder Kommunalbanken entsandte bzw. gewählte Mitglieder gelten im Sinne von Rz 24 als unabhängig, sofern sie: 25

- nicht der kantonalen oder kommunalen Regierung oder Verwaltung, respektive einer anderen kantonalen oder kommunalen Körperschaft des öffentlichen Rechts angehören, und 26
- von ihrem Wahlorgan keine Instruktionen für die Tätigkeit als Verwaltungsrat entgegennehmen. 27

C. Arbeitsteilung im Verwaltungsrat und Ausschüsse des Verwaltungsrats

Zu seiner Unterstützung kann der Verwaltungsrat Ausschüsse einrichten oder Aufgaben einzelnen Mitgliedern übertragen. 28

| | |
|--|----|
| Ab einer gewissen Grösse oder Komplexität des Instituts ist ein Audit Committee einzurichten (vgl. Rz 32–36). | 29 |
| Verfügt ein Institut über kein Audit Committee, so beauftragt der Verwaltungsrat ein oder zwei unabhängige und die Anforderungen von Rz 39 erfüllende Verwaltungsratsmitglieder, jedoch nicht den Verwaltungsratsvorsitzenden mit den Aufgaben gemäss Rz 41–53. Die FINMA kann Ausnahmen bewilligen. Wird der Verwaltungsratsvorsitzende mit den erwähnten Aufgaben beauftragt, so ist dies im Jahresbericht zu begründen. | 30 |
| Die an Ausschüsse oder einzelne Personen delegierten Aufgaben und Kompetenzen sowie entsprechenden Informations-, Abstimmungs-, und Berichterstattungspflichten sind vom Verwaltungsrat zu regeln. Die Verantwortung für die übertragenen Aufgaben verbleibt in jedem Fall beim gesamten Verwaltungsrat. | 31 |
| D. Audit Committee | |
| a) Kriterien bezüglich Einrichtung eines Audit Committee | |
| Die Institute richten ein Audit Committee (Prüfungsausschuss) ein, wenn mindestens eines der in den Rz 33–36 aufgeführten Kriterien zutrifft: | 32 |
| • Bilanzsumme > CHF 5 Mia. | 33 |
| • Depotvolumen (Wertschriften- und Edelmetallbestände von Kunden, ohne Banken, gemäss Aufsichtsreporting AU 001/AU 101) > CHF 10 Mia. | 34 |
| • Erforderliche Eigenmittel gemäss Eigenmittelverordnung (ERV) > CHF 200 Mio. | 35 |
| • Kotierung (Beteiligungstitel) | 36 |
| Richtet ein Institut trotz Zutreffen eines oder mehrerer Kriterien gemäss Rz 33–36 kein Audit Committee ein, so ist dies im Jahresbericht zu begründen. | 37 |
| b) Anforderungen an die Mitglieder eines Audit Committee | |
| Die Mehrheit der Mitglieder muss die Unabhängigkeitsanforderungen von Rz 20–24 erfüllen; Erfüllt weniger als die Mehrheit der Mitglieder die Anforderungen, so ist dies im Jahresbericht zu begründen. | 38 |
| Mitglieder des Audit Committee verfügen über gute Kenntnisse und Erfahrung im Finanz- und Rechnungswesen und sind mit der Tätigkeit der internen und externen Prüfer vertraut. | 39 |
| Der Vorsitzende des Verwaltungsrats soll dem Audit Committee nicht angehören. Entscheidet das Institut, dass dieser dem Audit Committee angehört, so ist dies im Jahresbericht zu begründen. | 40 |
| c) Aufgaben eines Audit Committee | |
| Das Audit Committee kann im Rahmen seiner Aufgaben Aufträge erteilen. | 41 |

aa) *Überwachung und Beurteilung der Integrität der Finanzabschlüsse*

Das Audit Committee

- analysiert kritisch die Finanzabschlüsse, d.h. die Einzel- und allfällige Konzernrechnung, die Jahres- und publizierten Zwischenabschlüsse, sowie die Erstellung in Übereinstimmung mit den angewendeten Rechnungslegungsgrundsätzen und beurteilt insbesondere die Bewertung der wesentlichen Bilanz- und Ausserbilanzpositionen; 42
- bespricht die Finanzabschlüsse sowie die Qualität der zugrunde liegenden Rechnungslegungsprozesse mit dem für das Finanz- und Rechnungswesen verantwortlichen Geschäftsführungsmitglied, mit dem leitenden Prüfer sowie mit dem Leiter der internen Revision; 43
- berichtet dem Verwaltungsrat über die gemäss Rz 42–43 vorgenommenen Arbeiten und gibt eine Empfehlung ab, ob der Eigentümerversammlung die Finanzabschlüsse vorgelegt werden können. Der Entscheid obliegt dem Gesamtverwaltungsrat. 44

bb) *Überwachung und Beurteilung der internen Kontrolle im Bereich der finanziellen Berichterstattung*

Das Audit Committee

- überwacht und beurteilt, ob die interne Kontrolle im Bereich der finanziellen Berichterstattung angemessen und wirksam ist; 45
- vergewissert sich, dass die interne Kontrolle im Bereich der finanziellen Berichterstattung bei wesentlichen Änderungen im Risikoprofil des Instituts entsprechend angepasst wird. 46

cc) *Überwachung und Beurteilung der Wirksamkeit der Prüfgesellschaft sowie deren Zusammenwirken mit der internen Revision*

Das Audit Committee

- würdigt einmal jährlich sowie bei wesentlichen Änderungen im Risikoprofil des Instituts die Risikoanalyse, die abgeleitete Prüfstrategie und den entsprechenden risikoorientierten Prüfplan der Prüfgesellschaft (FINMA-RS 08/41 „Prüfwesen“); 47
- analysiert kritisch die Prüfberichte über die Rechnungs- und Aufsichtsprüfung (vgl. FINMA-RS 08/41 „Prüfwesen“) und bespricht diese mit dem leitenden Prüfer; 48
- vergewissert sich, ob Mängel behoben bzw. Empfehlungen der Prüfgesellschaft umgesetzt werden; 49
- beurteilt die Leistung und Honorierung der Prüfgesellschaft und vergewissert sich über ihre Unabhängigkeit; 50
- beurteilt das Zusammenwirken von Prüfgesellschaft und interner Revision. 51

dd) *Beurteilung der über den Bereich der finanziellen Berichterstattung hinausgehenden internen Kontrolle und der internen Revision*

Das Audit Committee

- beurteilt die Funktionsfähigkeit der über den Bereich der finanziellen Berichterstattung hinausgehenden internen Kontrolle, namentlich der Compliance-Funktion und Risikokontrolle, soweit diese Beurteilung nicht durch andere Ausschüsse des Verwaltungsrats vorgenommen wird; 52
- muss über die Prüfergebnisse der internen Revision informiert werden und mit deren Leiter in regelmässigem Kontakt stehen, auch wenn die interne Revision aufgrund Rz 28 und 31 dem Gesamtverwaltungsrat oder einem anderen seiner Ausschüsse unterstellt ist. 53

IV. Interne Revision

A. Einrichtung

Jedes Institut hat eine interne Revision einzurichten (vgl. Art. 9 Abs. 4 BankV bzw. Art. 20 Abs. 2 BEHV). 54

In besonderen Fällen kann die FINMA, nach Anhörung der Prüfgesellschaft, ein Institut von der Verpflichtung gemäss Rz 54 befreien. 55

Erscheint die Einrichtung einer betriebseigenen internen Revision als nicht angemessen, können die Aufgaben der internen Revision übertragen werden: 56

- der internen Revision der Muttergesellschaft oder der internen Revision einer anderen Gruppengesellschaft, sofern diese eine Bank, ein Effekthändler oder ein anderer staatlich beaufsichtigter Finanzintermediär (z.B. Versicherungsunternehmen) ist (für ausländische Banken im Rahmen von Art. 4^{quinquies} BankG), 57
- einer zweiten Prüfgesellschaft, welche von der Prüfgesellschaft des Instituts unabhängig ist, oder 58
- einem unabhängigen Dritten, vorausgesetzt die Prüfgesellschaft bestätigt dessen professionelle Befähigung. 59

B. Unterstellung und Organisation

Die interne Revision ist dem Verwaltungsrat oder einem seiner Ausschüsse unmittelbar unterstellt und nimmt die ihr von diesem übertragenen Prüf- und Überwachungsaufgaben wahr. Die interne Revision berichtet in erster Linie dem Gremium des Verwaltungsrats, dem sie direkt unterstellt ist. 60

Die interne Revision der Finanzgruppe oder des Finanzkonglomerats erstreckt sich mindestens auf alle gemäss Art. 3b–3g BankG, Art. 10 Abs. 5 und 14 BEHG sowie Art. 6–10 ERV konsolidierungspflichtigen Unternehmen. Sofern selbständige Revisionsabteilungen bei Gruppengesellschaften bestehen, sind diese der internen Revision der Finanzgruppe oder des Finanzkonglomerats funktional zu unterstellen. 61

| | |
|---|----|
| Der Leiter der internen Revision wird vom Verwaltungsrat ernannt. | 62 |
| Die interne Revision arbeitet unabhängig von den täglichen Geschäftsprozessen. | 63 |
| Die interne Revision verfügt über ein unbeschränktes Prüfrecht innerhalb des Instituts und dessen konsolidierungspflichtigen Unternehmen gemäss Rz 61. Sie hat uneingeschränktes Zugriffsrecht auf sämtliche Bücher, Dokumente, Protokolle und andere Aufzeichnungen sowie Datenträger und Systeme. Es sind ihr alle Auskünfte zu erteilen, die zur Erfüllung ihrer Prüfungsaufgaben erforderlich sind. | 64 |
| Die für die interne Revision notwendigen Grundlagen, wie z.B. ein Reglement mit Angaben zu Organisation, Aufgaben und Verantwortlichkeiten, sind gemäss den unmittelbaren Unterstellungsverhältnissen vom Verwaltungsrat oder dem zuständigen Ausschuss zu erlassen. Daneben legt die interne Revision ihre Arbeitsweise (z.B. Methodik, Revisionsarten, Aus- und Weiterbildung) fest. | 65 |
| Die interne Revision hat die qualitativen Anforderungen des Schweizerischen Verbandes für interne Revision (SVIR) zu erfüllen. Ausnahmen sind im Jahresbericht zu begründen. Die Arbeit der internen Revision richtet sich nach den Standards for the Professional Practice des Institute of Internal Auditors (IIA). | 66 |
| Die interne Revision ist der Grösse, Komplexität und dem Risikoprofil des Instituts entsprechend auszugestalten und bildet organisatorisch eine selbständige Einheit. Sie muss personell ausreichend dotiert sein und über die nötigen Fachkompetenzen und Sachmittel (z.B. IT-Hilfsmittel) verfügen, damit sie ihr Mandat erfüllen kann. Das Kader muss über gründliche Kenntnisse in den Aktivitätsbereichen verfügen, in denen das Institut tätig ist. Insgesamt muss sichergestellt sein, dass die Ordnungsmässigkeit der Geschäftsführung und die Angemessenheit des internen Kontrollsystems mit qualifizierten Prüfern beurteilt werden. | 67 |
| Das Entschädigungssystem für Mitarbeiter der internen Revision darf keine Anreize setzen, die zu Interessenkonflikten führen. Insbesondere darf die Entschädigung (z.B. Löhne, Boni, Honorare, und Prämien) nicht vom Resultat einzelner Produkte und Transaktionen abhängen. | 68 |
| C. Aufgaben und Verantwortlichkeiten | |
| a) Risikobeurteilung, Prüfplanung und Berichterstattung | |
| Die interne Revision liefert wichtige Entscheidungsgrundlagen für die Beurteilung, ob das Institut ein dem Risikoprofil des Instituts angemessenes und wirksames internes Kontrollsystem besitzt. | 69 |
| Die interne Revision führt mindestens jährlich eine umfassende Risikobeurteilung des Instituts durch, wobei sie externe Entwicklungen (z.B. wirtschaftliches Umfeld, regulatorische Änderungen) und interne Faktoren (z.B. wesentliche Projekte, neue Geschäftsausrichtung) angemessen berücksichtigt. | 70 |
| Ausgehend von dieser Risikobeurteilung legt die interne Revision schwergewichtig die Prüfziele für die nächste Prüfperiode fest. | 71 |
| Im Weiteren stellt die interne Revision sicher, dass sämtliche risikorelevanten Geschäftsaktivitäten im Rahmen einer Mehrjahresplanung einer Prüfung durch sie selbst oder die Prüfgesell- | 72 |

schaft unterliegen.

Die interne Revision informiert den Verwaltungsrat oder den zuständigen Ausschuss und die Geschäftsführung schriftlich über die Risikobeurteilung und die Prüfziele und lässt die Prüfziele und Prüfplanung durch den Verwaltungsrat oder den zuständigen Ausschuss genehmigen. Sie stellt der Prüfgesellschaft eine Kopie der Unterlagen zu. 73

Während der Prüfperiode beurteilt die interne Revision, ob wesentliche Änderungen im Risiko- profil eingetreten sind und ob diese eine Anpassung der Prüfplanung erfordern. Allenfalls not- wendige wesentliche Anpassungen zur Jahresplanung unterbreitet sie zeitgerecht dem Verwal- tungsrat oder dem zuständigen Ausschuss zur Genehmigung. Sie informiert die Prüfgesell- schaft über solche Änderungen. 74

Die interne Revision erstattet zeitgerecht über alle wichtigen Feststellungen einer Prüfung schriftlich Bericht an den Verwaltungsrat oder den zuständigen Ausschuss und die Geschäfts- führung. 75

Mindestens jährlich erstellt die interne Revision einen schriftlichen Bericht über die wesentli- chen Prüfergebnisse und wichtigen Tätigkeiten in der Prüfperiode und unterbreitet diesen und die entsprechenden Schlussfolgerungen dem Verwaltungsrat oder dem zuständigen Aus- schuss zur Kenntnisnahme. Der Bericht ist auch der Geschäftsführung und der Prüfgesellschaft zuzustellen. 76

Im Weiteren informiert die interne Revision den Verwaltungsrat oder den zuständigen Aus- schuss mindestens halbjährlich über die Beseitigung festgestellter Mängel bzw. den Stand der Umsetzung von Empfehlungen der internen Revision und der Prüfgesellschaft. Diese Informa- tion und das entsprechende „Audit Tracking“ kann auch durch eine andere unabhängige In- stanz im Institut erfolgen, beispielsweise durch die Compliance-Funktion oder die Risikokontrol- le. 77

b) Abgrenzung zur Prüfgesellschaft

Die interne Revision und die Prüfgesellschaft koordinieren ihre Prüftätigkeit. Sie stimmen sich im Rahmen der Festlegung ihrer jeweiligen Prüfziele/-strategien ab. Sie vertreten dabei ihre je- weiligen Standpunkte und können darauf gestützt das gemeinsame Vorgehen festlegen. Die in- terne Revision bleibt für die Erfüllung ihrer Prüfziele verantwortlich. 78

Die interne Revision stellt der Prüfgesellschaft ihre Prüfberichte zeitgerecht zu. Die Prüfgesell- schaft hat das Recht, in die Arbeitspapiere der internen Revision Einsicht zu nehmen. Umge- kehrt stellt die Prüfgesellschaft ihre Prüfberichte der internen Revision zur Verfügung. 79

V. Geschäftsführung

A. Aufgaben und Verantwortlichkeiten

Die Geschäftsführung setzt die Vorgaben des Verwaltungsrats bezüglich Einrichtung, Aufrecht- erhaltung und regelmässiger Überprüfung der internen Kontrolle um. 80

Die Geschäftsführung

- entwickelt geeignete Prozesse für die Identifikation, Messung, Bewertung, Beurteilung und 81

Kontrolle der durch das Institut eingegangenen Risiken. Dies umfasst insbesondere die Konkretisierung der in die Arbeitsprozesse integrierten Kontrollaktivitäten gemäss Rz 87–96, der Compliance-Funktion gemäss Rz 100–112 und der Risikokontrolle gemäss Rz 113–125;

- hält eine Organisationsstruktur aufrecht, in welcher Verantwortlichkeiten, Kompetenzen, Rechenschaftspflichten, Anordnungs- und Entscheidungsbefugnisse sowie Informationsflüsse eindeutig festgelegt sind, und dokumentiert diese; 82
- stellt sicher, dass alle relevanten Informationen über das betriebliche Geschehen erhoben, verteilt und bearbeitet werden (Management Informationssystem); 83
- überprüft regelmässig die Angemessenheit der internen Kontrolle; 84
- berichtet periodisch an den Verwaltungsrat über die Wirksamkeit der internen Kontrolle und informiert den Verwaltungsrat und die interne Revision unverzüglich im Falle schwerwiegender Feststellungen. 85

B. Funktionentrennung und Kontrollaktivitäten

Die Geschäftsführung stellt eine geeignete Trennung von Funktionen sicher und vermeidet die Zuweisung konfliktärer Verantwortungen. In Fällen, in denen eine Funktionentrennung aufgrund der Unternehmensgrösse nicht vollständig umgesetzt werden kann, legt sie besonderen Wert auf eine entsprechend erhöhte Führungsverantwortung der Linieninstanzen. 86

Kontrollaktivitäten sind als integraler Bestandteil sämtlicher Arbeitsprozesse vorzusehen, beispielsweise als: 87

- Ablaufkontrollen: Diese stellen Zielabweichungen zu einem Zeitpunkt fest, bei dem Korrekturen noch leicht möglich sind. 88
- Ergebniskontrollen: Diese vergleichen Zielvorgaben mit den tatsächlich erreichten Resultaten. Sie werden eingesetzt, wenn unmittelbare Korrekturen nicht nötig und/oder nicht möglich sind. 89
- Verhaltensüberprüfungen: Mit diesen wird das Verhalten von Individuen und organisatorischen Einheiten überprüft. Sie werden insbesondere eingesetzt, wenn keine quantitativen Resultate beobachtbar sind. 90

Anzuwendende Kontrollaktivitäten sind u. a.: 91

- Aktivitätskontrollen: Die verschiedenen Führungsebenen sollen regelmässig stufengerechte Berichte zur wirtschaftlichen Leistung, Risiko- und Kontrollsituation erhalten und kritisch hinterfragen. 92
- Physische Kontrollen: Beispielsweise in Form des Vier-Augen-Prinzips, der Begrenzung des technischen Zugangs zu Barschaften und Wertgegenständen, der periodischen Inventarisierung. 93
- Überprüfung der Einhaltung vorgegebener Limiten. 94
- Überprüfung der Einhaltung von Kompetenzen und Autorisationen, insbesondere Überprü- 95

| | |
|---|-----|
| fung der Autorisationen bezüglich Zugang zu und Mutation von IT-Systemen und Stammdaten („golden-keyholders“). | |
| • Überprüfung und Abstimmung, beispielsweise von Transaktionen und Buchhaltungspositionen. | 96 |
| C. Compliance (Normeneinhaltung) | |
| Als Compliance gilt das Einhalten von gesetzlichen, regulatorischen und internen Vorschriften sowie die Beachtung von marktüblichen Standards und Standesregeln. | 97 |
| Als Compliance-Risiko gilt das Risiko von Verstössen gegen Vorschriften, Standards und Standesregeln und entsprechenden rechtlichen und regulatorischen Sanktionen, finanziellen Verlusten oder Reputationsschäden. | 98 |
| Die Geschäftsführung trägt die Verantwortung für die Umsetzung angemessener interner Systeme und Prozesse zur Gewährleistung der Compliance im Institut. Sie trifft die entsprechenden betrieblichen Massnahmen und Vorkehrungen, sorgt insbesondere für ein zweckmässiges Weisungswesen und ordnet die stufengerechte Einbindung aller Mitarbeiter in die Aufrechterhaltung der Compliance an. Bei international tätigen Instituten ist namentlich zu gewährleisten, dass Weisungen mit Wirkung für mehrere Länder mit dem lokalen Recht vereinbar sind. | 99 |
| D. Compliance-Funktion | |
| a) Einrichtung und Unterstellung | |
| Jedes Institut unterhält eine Compliance-Funktion, die im Rahmen ihrer Aufgaben ein uneingeschränktes Auskunfts-, Zugangs- und Einsichtsrecht hat und von ertragsorientierten Geschäftsaktivitäten unabhängig in die Gesamtorganisation einzugliedern ist. | 100 |
| Die Compliance-Funktion ist nach Massgabe der Grösse, der Geschäfts- und Organisationskomplexität und des Compliance-Risikos des Instituts mit angemessenen Ressourcen und Kompetenzen auszustatten. | 101 |
| Das Institut bestimmt ein Mitglied der Geschäftsführung, das für die Compliance-Funktion zuständig ist, und gewährleistet damit einen ungehinderten Zugang der Compliance-Funktion zur Geschäftsführung. | 102 |
| Das Entschädigungssystem für Mitarbeiter der Compliance-Funktion darf keine Anreize setzen die zu Interessenkonflikten führen. Insbesondere darf die Entschädigung (z.B. Löhne, Boni, Honorare und Prämien) nicht vom Resultat einzelner Produkte und Transaktionen abhängen. | 103 |
| Die Compliance-Funktion kann mit anderen internen Funktionen, mit welchen keine Interessenkonflikte bestehen, eine Abteilung bilden, z.B. mit dem Rechtsdienst oder der Risikokontrolle, wobei die Aufgaben jeder einzelnen Funktion klar zu definieren und zuzuordnen sind. | 104 |
| Namentlich bei geringer Geschäfts- und Organisationskomplexität und tiefem Compliance-Risiko kann die Compliance-Funktion auch in Teilzeitarbeit oder in Personalunion mit einer anderen internen Funktion, mit welcher keine Interessenkonflikte bestehen, oder in einem Outsourcing-Verhältnis betrieben werden. | 105 |
| Kann in kleinen Instituten aufgrund der Grössenverhältnisse die geforderte unabhängige Ein- | 106 |

gliederung der Compliance-Funktion gemäss Rz 100 und Abwesenheit von Interessenkonflikten gemäss Rz 105 nicht vollständig gewährleistet werden, so ist die zuverlässige Wahrnehmung der Aufgaben einer Compliance-Funktion anderweitig sicherzustellen. Die Prüfgesellschaft hat dies zu beurteilen und nimmt jeweils Stellung im Bericht über die Aufsichtsprüfung.

b) Aufgaben und Verantwortlichkeiten

Aufgaben, Verantwortlichkeiten und Berichterstattung der Compliance-Funktion sind in einer Regelung festzuhalten, die von der Geschäftsführung oder dem Verwaltungsrat zu genehmigen ist. 107

Die Aufgaben der Compliance-Funktion umfassen in der Regel:

- Unterstützung und Beratung der Geschäftsführung sowie der Mitarbeiter bei der Durchsetzung und Überwachung der Compliance; 108
- Mindestens jährliche Einschätzung des Compliance-Risikos der Geschäftstätigkeit des Instituts und Ausarbeitung eines risikoorientierten Tätigkeitsplans, der durch die Geschäftsführung zu genehmigen ist. Der Tätigkeitsplan ist auch der internen Revision zur Verfügung zu stellen; 109
- Unterstützung der Geschäftsführung bei der Ausbildung und Information der Mitarbeiter bezüglich Compliance; 110
- Zeitgerechte Berichterstattung an die Geschäftsführung über wesentliche Veränderungen in der Einschätzung des Compliance-Risikos, Feststellung und Untersuchung von schwerwiegenden Verletzungen der Compliance und Unterstützung der Geschäftsführung bei der Wahl der zu treffenden Anordnungen oder Massnahmen. Die interne Revision ist entsprechend zu informieren; 111
- Jährliche Berichterstattung an den Verwaltungsrat über die Einschätzung des Compliance-Risikos und die Tätigkeit der Compliance-Funktion gemäss Rz 108–111. Eine Kopie der Berichterstattung ist der internen Revision und der Prüfgesellschaft zur Verfügung zu stellen. 112

E. Risikokontrolle

a) Einrichtung und Unterstellung

Jedes Institut unterhält eine Risikokontrolle, die im Rahmen ihrer Aufgaben ein uneingeschränktes Auskunfts-, Zugangs- und Einsichtsrecht hat und von ertragsorientierten Geschäftsaktivitäten unabhängig in die Gesamtorganisation einzugliedern ist. 113

Die Risikokontrolle ist nach Maßgabe der Größe, der Geschäfts- und Organisationskomplexität und des Risikoprofils eines Instituts mit angemessenen Ressourcen und Kompetenzen auszustatten. 114

Das Institut bestimmt ein Mitglied der Geschäftsführung, das für die Risikokontrolle zuständig ist, und gewährleistet damit einen ungehinderten Zugang der Risikokontrolle zur Geschäftsführung. 115

Entsprechend den verschiedenen Risikokategorien des Instituts (z.B. Markt-, Kredit-, operatio- 116

nelle Risiken) kann die Risikokontrolle aus verschiedenen selbständigen Abteilungen oder Stellen bestehen, welche jedoch alle an das für die Risikokontrolle zuständige Mitglied der Geschäftsführung rapportieren.

Das Entschädigungssystem für Mitarbeiter der Risikokontrolle darf keine Anreize setzen die zu Interessenkonflikten führen. Insbesondere darf die Entschädigung (z.B. Löhne, Boni, Honorare und Prämien) nicht vom Resultat einzelner Produkte und Transaktionen abhängen. 117

Die Risikokontrolle kann mit anderen internen Funktionen, mit welchen keine Interessenkonflikte bestehen (z.B. mit der Compliance-Funktion), eine Abteilung bilden, wobei die Aufgaben jeder einzelnen Funktion klar zu definieren und zuzuordnen sind. 118

Namentlich bei geringer Geschäfts- und Organisationskomplexität und tiefem Risikoprofil kann die Risikokontrolle auch in Teilzeitarbeit oder in Personalunion mit einer anderen internen Funktion, mit welcher keine Interessenkonflikte bestehen, betrieben werden. 119

Kann in kleinen Instituten aufgrund der Grössenverhältnisse die geforderte unabhängige Eingliederung der Risikokontrolle gemäss Rz 113 und Abwesenheit von Interessenkonflikten gemäss Rz 119 nicht vollständig gewährleistet werden, so ist die zuverlässige Wahrnehmung der Aufgaben einer Risikokontrolle anderweitig sicherzustellen. Die Prüfgesellschaft hat dies zu beurteilen und nimmt jeweils Stellung im Bericht über die Aufsichtsprüfung. 120

b) Aufgaben und Verantwortlichkeiten

Aufgaben, Verantwortlichkeiten und Berichterstattung der Risikokontrolle sind in einer Regelung festzuhalten, die von der Geschäftsführung oder vom Verwaltungsrat zu genehmigen ist. 121

Die Risikokontrolle überwacht als unabhängige Kontrollfunktion das eingegangene Risikoprofil des Instituts. Sie stellt die für die Risikoüberwachung notwendigen Risikoinformationen bereit und legt die Grundlage der unternehmerischen Risikopolitik (Risk Policy), der Risikobereitschaft (Risk Appetite) sowie der Risikolimiten, die von der Geschäftsführung oder dem Verwaltungsrat zu genehmigen sind. 122

In die Verantwortlichkeit der Risikokontrolle fallen insbesondere die Gestaltung und Umsetzung von adäquaten Risikoüberwachungssystemen und deren Anpassung an neue Geschäfte und Produkte, die Vorgabe und Anwendung von Grundlagen und Methoden für die Risikomessung (z.B. Bewertungs- und Aggregationsmethoden, Validierung von Modellen) sowie die Überwachung angemessener Systeme für die Berücksichtigung der Eigenmittel-, Risikoverteilungs- und Liquiditätsvorschriften. 123

Die Risikokontrolle erstattet der Geschäftsführung mindestens halbjährlich einen Bericht über die Risiken bzw. Risikopositionen. Bei besonderen Entwicklungen informiert sie unverzüglich die Geschäftsführung und die interne Revision. 124

Die Risikokontrolle berichtet dem Verwaltungsrat mindestens jährlich über die Risikolage des Instituts und ihre Tätigkeit gemäss Rz 122–124. Eine Kopie der Berichterstattung ist der internen Revision und der Prüfgesellschaft zur Verfügung zu stellen. 125

c) Abgrenzung zum Risikomanagement

Das Risikomanagement bezweckt die umfassende und systematische Steuerung und Lenkung von Risiken auf der Grundlage wirtschaftlicher und statistischer Kenntnisse. Risikomanagement umfasst die Identifikation, Messung, Beurteilung, Steuerung und Berichterstattung über einzel- 126

ne wie auch über aggregierte Risikopositionen. Risikomanagement erfolgt mit adäquaten und den Besonderheiten des Instituts Rechnung tragenden Methoden auf den jeweils geeigneten organisatorischen Ebenen.

VI. Prüfung und Beurteilung durch die Prüfgesellschaften

Die bankengesetzlichen Prüfgesellschaften prüfen die Einhaltung dieses Rundschreibens nach Massgabe des FINMA-RS 08/41 „Prüfwesen“ und halten das Ergebnis ihrer Prüfungshandlungen im Prüfbericht fest. 127